UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/050,752	01/16/2002	Sean Brennan	16375-00025	7828

21186 7590 01/17/2007

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	01/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/050,752
Filing Date: January 16, 2002
Appellant(s): BRENNAN, SEAN

Thomas F. Brennan
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed October 16, 2006 appealing from the Office action mailed April 14, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,853,980 YING et al. 2-2005

Tan et al. US Patent Application Publication 2001/0045451 A1, 11-2002.

Krueger et al. US Patent Application Publication 2002/0077837 A1, 6-2002.

Aladdin. "eToken: The Key to Security for the Internet Age", July 2000.

RSA Security, Inc. "RSA Web Security Portfolio - How RSA SecurID Agents Can Secure Your Website", August 2000.

Stallings, William. Network Security Essentials, Applications and Standards, Prentice-Hall, Inc., pp. 203-223.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 4-5, 7-9, 18, 21 & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,853,980 to Ying et al. (**Ying**) and U.S. Patent Application Publication 2002/0077837 to Krueger et al. (**Krueger**).

Regarding claims 4-5, 7-9 & 18, Ying teaches providing a first user authentication method (col. 23, lines 23-37) and a second authentication method (col. 23, lines 43-46), wherein the first and second user authentication methods are selected to authenticate at least one factor associated with the user/password and credit card information (col. 23, lines 23-37), enabling a user to communicate authentication data to a first web site using the Internet (col. 23, lines 23-50), authenticating the user at the first web site using the first authentication method/user and password (col. 23, lines 23-37), enabling the communication of at least some of the authentication data/credit card information from the first web site to a second web site/credit card processor (col. 23, lines 52-63) using the second authentication method/credit card processing, and wherein both web sites (font web site and credit card processor) are involved in user authentication using the authentication data and wherein access to content/fonts on the first web site is restricted if the user is not authenticated to both web sites (col. 23, line 65 – col. 24, line

5). Ying discloses a second server/credit card processor, but lacks specifically a web site. However, Krueger teaches a first web site/merchant web page (¶40) where authentication information/user and password information and credit card information is entered and transferred from a first web site to an authentication web site/verification system (¶41), wherein the user authenticates a second web site/verification system (¶¶43-44) to gain the benefit of increased security of the user's confidential information (¶9). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to make use of Krueger's system, and as such include credit card information to be sent from Ying's font web site to Krueger's verification system web site, as part of the checkout process, where the user is further authenticated to the verification system web site/verification system web site. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information, as taught by Krueger (¶9). See also ¶10.

Regarding claim 21, Ying discloses requiring a user authenticate to a first web site/merchant web site (col. 23, lines 9-37), where the user is granted access to content if authenticated (col. 23, line 65 – col. 24, line 5). Ying's system discloses that once the user is authenticated to the first web site/font web site, the user engages in a credit or debit checkout (col. 23, lines 41-50), but lacks authenticating to a second web site. However, Krueger teaches a first web site/merchant web page (¶40) and authenticating the user to a second web site/verification system (¶¶43-44) to gain the benefit of increased security of the user's confidential information (¶9). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying such that once authenticated to

the first web site/merchant web site, authenticate the user to a second web site/verification system site, where the user is granted access to content on the first web site only if authenticated to both the first and second web sites. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information, as taught by Krueger (¶¶9, 43-44 & 61-63). See also ¶10.

Regarding claim 28, Ying discloses a first web site/merchant web site (col. 23, lines 9-37), implementing a first authentication method (user/pass), entering authentication information/credit card information and user/password information (col. 23, lines 23-26 & 41-50) via the first web site/merchant web site wherein the user is granted access to content on the first web site/merchant web site only if authenticated to both the first web site and a credit card processor (col. 23, line 41 – col. 24, line 5). Ying lacks an authentication web site implementing a second authentication method, connected to the first web site where authentication information for the second authentication method is transferred from the first web site to the authentication web site and granting access only if the user is authenticated to both the first web site and a second web site. However, Krueger teaches a first web site/merchant web page (¶40) where authentication information/credit card information is entered and transferred from a first web site to an authentication web site/verification system (¶41), wherein the user authenticates a second web site/verification system (¶¶43-44) to gain the benefit of increased security of the user's confidential information (¶9). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to make use of Krueger's system, and as such include credit card information to be sent from Ying's font web site to Krueger's verification system web site, as part of the checkout process, where the user is further

authenticated to the verification system web site. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information, as taught by Krueger (¶9). See also ¶10.

2. Claims 10-12, 19-20, 22-27 & 29-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ying** and **Krueger**, as applied to claims 21 & 28 above, in further view of "RSA Web Security Portfolio, How RSA SecurID Agents Can Secure Your Website" by **RSA**.

Regarding claims 10-12, Ying lacks one authentication method employing a password. However, RSA teaches that two-factor authentication (p. 2, ¶1), which comprises entering a user ID, PIN and a randomly generated authentication code generated by a token (p. 2, ¶4), ensures greater security than traditional static passwords (p. 2, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying such that the user enters at least a randomly generated authentication code to Ying's font web site, and hence authenticates to the web site using a token. One of ordinary skill in the art would have been motivated to perform such a modification to ensure greater security, as taught by RSA (p. 2, ¶¶1-4).

Regarding claim 19, Ying lacks at least one user authentication method used across multiple web sites. However, RSA teaches using the RSA SecurID system in a mixed Web server environment, where users can traverse between the servers without being re-authenticated by issuing cookies that are valid on multiple servers (p. 3, §Web Single Sign-on). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to utilize RSA SecurID to issue at least one cookie that is valid on multiple

servers. One of ordinary skill in the art would have been motivated to perform such a modification to enable users to traverse between the servers without being re-authenticated by issuing cookies that are valid on multiple servers, as taught by RSA (p. 3, §Web Single Sign-on).

Regarding claim 20, Ying lacks explicitly the token being embedded in a cell phone. However, RSA discloses embedding the token in a device such as a cell phone to fit with daily work habits (p. 2, §III, ¶5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying, as modified above, to include the token in a cell phone. One of ordinary skill in the art would have been motivated to perform such a modification because it is known to fit daily work habits, as taught by RSA (p. 2, §III, ¶5).

Regarding claims 22-24 & 29-31, Ying lacks authenticating to the second web site with a token. However, RSA teaches that two-factor authentication (p. 2, ¶1), which comprises entering a user ID, PIN and a randomly generated authentication code generated by a token (p. 2, ¶4), ensures greater security than traditional static passwords (p. 2, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying, as modified above, such that the user enters at least a randomly generated authentication code to Krueger's verification server, and hence authenticates to the second web site using a token. One of ordinary skill in the art would have been motivated to perform such a modification to ensure greater security, as taught by RSA (p. 2, ¶¶1-4).

Regarding claims 25-27 & 32-34, Ying lacks authenticating to the first web site with a first token and authenticating to the second web site with a second token. However, RSA teaches that two-factor authentication (p. 2, ¶1), which comprises entering a user ID, PIN and a

randomly generated authentication code generated by a token (p. 2, ¶4), ensures greater security than traditional static passwords (p. 2, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying to use RSA two-factor authentication and Krueger to use RSA two-factor authentication. One of ordinary skill in the art would have been motivated to perform such a modification to ensure greater security in both authentication systems, as taught by RSA (p. 2, ¶¶1-4).

3. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Ying, Krueger & RSA**, as applied to claim 11 above, in further view of U.S. Patent Application Publication 2001/0045451 to Tan et al. (**Tan**) in further view of "eToken: The Key to Security for the Internet Age" by **Aladdin**. RSA lacks explicitly a USB-based token being accessed by a browser. However, Tan teaches that to allow access to a web site using a smart card, the browser can read necessary access information directly from the smart card and pass the information to the server to which the user is authenticating (¶6-11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the RSA security token to communicate electronically with the web browser. One of ordinary skill in the art would have been motivated to perform such a modification to pass the generated code to the server for use in authentication, as taught by Tan (¶6-11). Further, Aladdin teaches that using USB tokens for authentication allows the user to take advantage of the USB ports included in millions of PCs (p. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify RSA to include the SecurID token in a USB-based device. One of ordinary skill in the art would have been motivated to perform such a

modification to take advantage of millions of USB-ready PCs for authentication, as taught by Aladdin (p. 1).

4. Claims 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ying**, **Krueger & RSA**, as applied to claim 4 above, in further view of Network Security Essentials Applications and Standards by **Stallings**. Ying, as modified above by RSA, lacks explicitly that the authentication method employs a fixed complex code that comprises a public key infrastructure. However, RSA discloses that the authentication token is transmitted using SSL (p. 3, §III, ¶2). Further, Stallings teaches that SSL involves a key exchange, for instance RSA key exchange, where a secret key is encrypted with the receivers RSA public key (p. 214). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to explicitly employ a fixed complex code that comprises a public key infrastructure. One of ordinary skill in the art would have been motivated to perform such a modification to utilize an RSA public key to exchange keys, as taught by Stallings (p. 214).

(10) Response to Argument

Appellant's brief (p. 12) argues that neither Ying nor Krueger teaches an authentication method and system using at least two different factors at two or more web sites. Appellant continues the argument on p. 13 by stating that in security, there are three authentication factors: what you know, what you have and what you are, each one being a single factor of authentication. Appellant argues that (p. 14) the credit card processor does not authenticate the user. However, it is submitted that Ying discloses two factors of authentication such that a first

factor (user name and password, col. 23, lines 23-27) is used to authenticate the user to the store and a second factor (credit card information, col. 23, lines 43-46) is used to authenticate the user to the credit card processor (second entity). The credit card information represents "something you have" and is expected, by one having ordinary skill in the art, to only be held by the user. Further, however, Krueger teaches that to enhance security (by not divulging all credit information to a merchant site, ¶¶9-10), the user is re-directed to a verification system of the credit processor (¶43) where the verification system requests information from the card (what the user knows, such as a PIN or what the user has, something from the card itself, ¶44) to complete the transaction, thus authenticating the user while not divulging the credit information.

Appellant's brief (p. 13) argues that Ying does not describe two-factor authentication occurring at two-different web sites (or servers). However, Ying discloses a first authentication method (user name and password) occurring at a first web site or server (merchant web site, col. 23, lines 23-37) and a second authentication method (credit card processing) occurring at a second web site or server (col. 23, lines 43-46). In combination with Krueger, Ying discloses the credit card processing requesting a PIN (something a user knows) or information from a credit card (something a user has) explicitly authenticating the user at a second web site (¶¶40-44).

Appellant's brief (p. 15) argues that Ying's credit card information is not "what the user has". However, it is submitted that by requesting the information on the credit card, the credit card does represent what the user has. As explained above, Krueger teaches that to enhance security (by not divulging all credit information to a merchant site, ¶¶9-10), the user is re-directed to a verification system of the credit processor (¶43) where the verification system requests information from the card (what the user knows, such as a PIN or what the user has,

something from the card itself, ¶44) to complete the transaction, thus authenticating the user while not divulging the credit information. In combination, the user authenticates to two websites (the font merchant's web site of Ying and the verification system web site of Krueger) and can only access the data if authenticated to both web sites. The user only has access to the data if he/she is authenticated to both the merchant site and the credit-processing site, such that the data can be purchased (Ying, col. 23, lines 58-60 and Krueger, ¶¶45-48).

Appellant's brief (p. 15, ¶3) argues that Ying discloses at most, one factor of the same type and Ying therefore, does not describe "enabling a user to communicate authentication data for both authentication methods to a first web site" and "enabling the communication of at least some of the authentication data from the first web site to a second web site". However, the claims do not recite that the factors being different, such as for instance, one factor being what the user has and the other being what the user knows. However, even in such a case, the user name and password is something a user knows and the credit card information is something a user has. As modified by Krueger, Ying requests the user name, password and credit card information to the merchant web site (first web site) and (Krueger) requests further credit card information to the verification system website (second web site) where some information (credit card information) is passed from the first web site to the second web site (merchant web site, in this case a font merchant, to the verification system web site, see Ying, col. 23, lines 23-27, lines 43-46 and see Krueger, ¶¶40-44). This corresponds to the limitations "enabling a user to communicate authentication data for both authentication methods to a first web site" and "enabling the communication of at least some of the authentication data from the first web site to a second web site".

Appellant's brief (p. 16) argues that the PIN and credit card information represent "what the user knows", which is, in Appellant's words "another single-factor". In response, it is noted that a PIN is something a user knows and information read from a card is something a user has. Second, the claims recite "two-factor", and the user name and password of Ying, in combination of the PIN or information read from the users credit card of Krueger represents two-factor authentication.

Appellant's brief (p. 16) argues that neither Ying nor Krueger teach the first web site communicating with the second web site only if the user is initially authenticated. However, attention is directed to col. 23, lines 31-35, where the user name and password are verified, and "if so" (col. 23, line 34), the checkout page (credit card page) is downloaded.

Appellant's brief (p. 16) argues that neither Ying nor Krueger teach the first web site communicating to the second web site at least data relating to the second authentication method. However, attention is directed to Ying, col. 23, lines 43-60 where the credit card information is obtained and sent to a credit card processor. Further, Krueger teaches that the merchant system (the first web site) establishes a communications channel with the verification system (credit card processor) and sends the card number, merchant ID and the transaction amount (¶41). Therefore, Ying as modified above by Krueger, teaches at least part of the information used for the second authentication (credit card number) is sent from the first web site (Ying's font web site which corresponds to Krueger's merchant system) to the second web site (Ying's credit card processor which corresponds to Krueger's credit verification system).

Appellant's brief (p. 17) argues that neither Ying nor Krueger teaches a system that authenticates a user not only in the first site, but also in the second site. However, this limitation has been discussed in the previous paragraphs of this Answer.

Appellant's brief (p. 17) argues that there is no motivation to combine a reference that verifies a user's card information at a second server (Ying) with a reference that employs a card verification method over two web sites (Krueger) to form a method and system that authenticates a user not only in the first web site but also in the second web site. However, as discussed above, Krueger's system provides Ying's system a benefit, obvious to one having ordinary skill in the art at the time the invention was made, such that when the credit card number from Ying is entered the remaining verification information is entered at the verification system web site. This serves two obvious purposes. First, the user is authenticated by a memorized PIN and optionally data read from the card, verifying that the user is who the user says they are and is in possession of the card. Second, all the information is not entered at the first web site so if the transaction to the first web site is intercepted, the interceptor will not receive all the necessary information. For at least these two security-enhancing benefits, motivation exists to combine verification system of Krueger to the credit processing part of Ying.

Appellant's brief (p. 18) argues that RSA fails to show two-factor authentication where both web sites are involved in user authentication using at least one authentication data of a different factor and where access to content on the first web site is restricted if the user is not authenticated to both web sites. However, RSA teaches that tokens (using a one-time PASSCODE, for example) are more secure than traditional static passwords (p. 2, ¶¶1-4). Therefore, one having ordinary skill in the art at the time the invention was made would have

been motivated to modify Ying such that the user employs a token to enter a PASSCODE into Ying's font web site rather than a static password, for the benefit of increased security, as taught by RSA. It should be noted that the Examiner is not suggesting replacing Ying's entire authentication system (combined password and credit processing) with RSA's invention (as Appellant implies on p. 18, ¶¶2-3 of the brief), but rather using RSA to enhance the security of the username and password portion of Ying.

Appellant's brief (p. 19) argues that RSA provides no motivation for combining one authentication method using a password at a first web site (Ying and Krueger) with another authentication method using a token (RSA) or one-time password at a second web site to form what is claimed. However, Appellant again appears to be referring to the misconception that Examiner is suggesting replacing Ying's entire authentication system (combined password and credit processing) with RSA's invention. Rather, the Examiner is suggesting that one having ordinary skill in the art would have found it obvious to instead of using the user name and password suggested by Ying, to employ a token as the password as described in RSA to enhance the security (one example being that a token value changes and cannot be memorized by an adversary as a password can) of the Ying password system. Ying's invention is not modified in any other way (after authentication of the token value entered, the process continues to request credit card information, i.e. authentication information for the second site).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael J. Simitoski

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron

Matthew Smithers